FINGERPRINT-BASED CRIMINAL HISTORY RECORD INFORMATION CHECKS MADE FOR NON-CRIMINAL JUSTICE PURPOSES Policy

EFFECTIVE: 3.19.26

This policy is applicable to any fingerprint-based state and national criminal history record check made for non-criminal justice purposes and requested under applicable federal authority and/or state statute authorizing such checks for educational employment and/or volunteer purposes. Where such checks are allowable by law, the following practices and procedures will be followed.

I. Requesting CHRI checks

Fingerprint-based CHRI checks will only be conducted as authorized by the FBI and Vermont Crime Information Center (VCIC), in accordance with all applicable state and federal rules and regulations. If an applicant or employee is required to submit to a fingerprint-based state and national criminal history record check, they shall be informed of this requirement and instructed on how to comply with the law. Such instruction will include information on the procedure for submitting fingerprints. In addition, the applicant or employee will be provided with all information needed to successfully register for a fingerprinting appointment.

II. Access to CHRI

All CHRI is subject to strict state and federal rules and regulations. CHRI is used only for the official purpose for which it was requested, and CHRI cannot be shared with other entities for any purpose, including subsequent hiring determinations. All receiving entities are subject to audit by the VCIC and the FBI, and failure to comply with such rules and regulations could lead to sanctions. Furthermore, an entity can be charged with federal and state crimes for the willful, unauthorized disclosure of CHRI.

III. CHRI Training

An informed review of a criminal record requires training. Accordingly, all personnel authorized to receive and/or review CHRI at Connected Circles will review and become familiar with the educational and relevant training materials regarding CHRI laws and regulations made available by the appropriate agencies.

In addition to the above, all personnel authorized to receive and/or review CHRI must undergo Security Awareness Training on an annual basis. This training will be accomplished using the training provided by CJIS Online.

IV. Adverse Decisions Based on CHRI

If inclined to make an adverse decision based on an individual's CHRI, Connected Circles will take the following steps prior to making a final adverse determination:

- Provide the individual the opportunity to complete or challenge the accuracy of their CHRI; and

- Provide the individual with information on the process for updating, changing, or correcting CHRI.

A final adverse decision based on an individual's CHRI will not be made until the individual has been afforded a reasonable time of 30 days to correct or complete the CHRI.

V. Point of Contact (POC) and Local Agency Security Officer (LASO)
Each NCJA receiving CHRI is required to designate a POC and a LASO.

The Connected Circles POC is Krista Metivier. The POC is responsible for the following:

- Ensuring all authorized personnel
  - Complete the appropriate level of CJIS Security Awareness Training in CJIS Online
  - Sign an Acknowledgement Statement of Misuse
- Inform the VCIC of changes in the agency head or any relevant business information (agency name changes, mailing/physical address changes, etc.)
  - Contact the VCIC immediately to update the User Agreement and, if necessary, submit the new authorization to the VCIC

The Connected Circles LASO is Krista Metivier. The LASO is responsible for the following:

- Identifying who is using or accessing CHRI and/or systems with access to CHRI
- Ensuring that personnel security screening procedures are being followed as stated in this policy
- Ensuring the approved and appropriate security measures are in place and working as expected
- Terminate access to CHRI immediately upon notification of an individual's termination of employment

VI. Retention of CHRI
Federal law prohibits the repurposing or dissemination of CHRI beyond its initial requested purpose. Once an individual's CHRI is received, it will be securely retained in internal agency documents for the following purposes only:

- Historical reference and/or comparison with future CHRI requests
- Dispute of the accuracy of the record
- Evidence for any subsequent proceedings based on information contained in the CHRI.

CHRI will be kept for the above purposes in:

- Hard copy form in personnel files located in the locked filing cabinet located in the locked filing room
  - CHRI will be retained for a minimum of three (3) years. At the end of this term, the CHRI will be disposed of according to the Disposal of Physical Media policy

VII. Storage of CHRI
CHRI shall only be stored for extended periods of time when needed for the integrity and/or utility of an individual's personnel file. Administrative, technical, and physical safeguards, which are in compliance with the most recent FBI security Policy, have been implemented to ensure the security

and confidentiality of CHRI. Each individual involved in the handling of CHRI is to familiarize themselves with these safeguards.

In addition to the above, each individual involved in the handling of CHRI will strictly adhere to the policy on the storage and destruction of CHRI.

VIII. Media/Physical Protection

All media containing CHRI is to be protected and secured at all times. The following is established and to be implemented to ensure the appropriate security, handling, transporting, and storing of CHRI media in all its forms.

Physical Storage and Access

Physical CHRI media shall be securely stored within physically secured locations or controlled areas. Access to such media is restricted to authorized personnel only and shall be secured at all times when not in use or under the supervision of an authorized individual.

Physical CHRI media:

- Is to be stored within employee records or by itself when necessary
- Is stored in a locked filing cabinet that only the Agency Head and POC/ LASO have keys for, in a room that is regularly locked, within an office suite that is locked.

IX. Destruction of CHRI

Disposal of Physical Media

Once physical CHRI media (paper/hard copies) is determined to be no longer needed by Connected Circles, it shall be destroyed and disposed of appropriately. Physical CHRI media shall be destroyed by shredding, cross-cut shredding, or incineration. Connected Circles will ensure such destruction is witnessed or carried out by authorized personnel:

- The LASO shall witness or conduct disposal
- Cross-cut shredding will be the method of destruction used by Connected Circles

X. Disciplinary

If an individual at Connected Circles has misused or is currently misusing CHRI, the following requirements will be adhered to.

- Using CHRI for any purpose other than what is allowed by state statute or Federal code is considered misuse
- Misuse of CHRI can result in loss of access to CHRI, loss of employment and/or criminal prosecution
- Misuse of CHRI shall be reported to the state

XI. Incident Response

The security of information and systems in general, and of CHRI in particular, is a top priority for Connected Circles. Therefore, we have established appropriate operational incident handling procedures for instances of an information security breach. It is each individual's responsibility to adhere to established security guidelines and policies and to be attentive to situations and incidents

which pose risks to security. Furthermore, it is each individual's responsibility to immediately report potential or actual security incidents to minimize any breach of security or loss of information. The following security incident handling procedures must be followed by each individual:

- All incidents will be reported directly to the LASO as soon as practical
- If any records were stolen, the incident will also be reported to appropriate authorities
- Once the cause of the breach has been determined, disciplinary measures will be taken in accordance with the disciplinary policy

In addition to the above, the LASO shall report all security-related incidents to the VCIC as soon as practical and submit an incident response form.

All agency personnel with access to FBI and/or VCIC CHRI have a duty to protect the system and related systems from physical and environmental damage and are responsible for correct use, operation, care and maintenance of the information. All existing laws and Connected Circles regulations and policies apply, including those that may apply to personal conduct. Misuse or failure to secure any information resources may result in temporary or permanent restriction of all privileges up to employment termination.